enterasys®

50 Minuteman Road
Andover, MA 01810 (USA)
Tel: (978) 684-1000

CUSTOMER RELEASE NOTES

Enterasys RoamAbout® Wireless Switch 8xx0 Release
Firmware Version 7.0.7.3
January 21, 2009

INTRODUCTION:

The RBT-8xx0 family of wireless switches include the following: 1) the RBT-8100 and RBT-8110, which have the ability to control up to 24 access points; 2) the RBT-8200 and RBT-8210, which have the ability to control 24/48/72 access points; 3) the RBT-8400, which has the ability to control 40/80/120 access points; and 4) the new RBT-8500 which can control 32/64/96/128 access points. The RoamAbout Switch Manager (RASM) can manage all of these devices.

The 7.0.7.3 Firmware release addresses firmware modifications and customer escalations (refer to *the Firmware and Enhancements* section).

Enterasys recommends that you thoroughly review this document prior to installing or upgrading this product.

NOTE: The following table provides the access points and features supported by the Wireless Switch 8xx0 Firmware Version 7.0.7.3

Access Point	Supported in 7.0.7.3	Hitless Failover	Direct Path Forwarding	Wireless Mesh Support
RBT3K-AG	Yes	No	No	No
RBT-1002	Yes	No	No	No
RBT-1002-EU	Yes	No	No	No
RBT-1602	Yes	Yes	No	No
RBT-4102	Yes	No	No	No
RBT-4102-EU	Yes	No	No	No
RBT-4102-BG	Yes	No	No	No
TRPZ-MP-372-CN	Yes	Yes	No	No
TRPZ-MP-372-IL	Yes	Yes	No	No
TRPZ-MP-422	Yes	Yes	Yes	Yes
TRPZ-MP-432	Yes	Yes	Yes	Yes (802.11a/b/g only)
TRPZ-MP-620	Yes	Yes	Yes	Yes

NOTE: Enabling Direct Path Forwarding (also known as local switching) for a given AP affects the number of ACEs that can be applied within a single ACL policy to a user connecting to that AP. When local switching is enabled on an AP in version 6.0.5.1 or greater of RAS firmware, up to 25 ACEs in an ACL policy can be applied to a user of that AP. Please refer to the *Firmware Changes and Enhancements* section for more information.

NOTE: To avoid conflicts with internal RAS VLAN numbering schemes, it is strongly advised to use VLAN IDs less than 3520 on RBT-8xxx systems that are upgrading from MSS version 6.0 to 7.0. Failure to do so will result in a loss of configuration data.

NOTE: RoamAbout Wireless Switch Firmware version 5.0.9.2 and greater supports the RBT-8210, the small form factor switch that replaces the larger RBT-8200. The RBT-8210 uses the RBT-8200 firmware and commands. The RBT-8210 prompt displays as RBT-8200.

NOTE: If you are using a 4.x firmware image/software, Enterasys recommends that you upgrade the RoamAbout Switch Manager (RASM) to firmware version 5.0.12.2 BEFORE upgrading your RBT-8xx0 wireless switches to firmware version 5.0.12.2. Please refer to the *Upgrading the RBT8xxx switches* **section of this release note for more information.**

NOTE: If you are upgrading a pre-existing RBT-4102 or RBT-4102-EU model Access Point from 4.1.4 or earlier, please read the instructions listed in the *Firmware Release 4.1.5.0* section of the *Firmware Changes and Enhancements* section of the RoamAbout Switch Manager (RASM) 6.2.2.4 Release Notes.

NOTE: RoamAbout Wireless Switch Firmware version 6.0.4.2 and greater replaces the term 'DAP' with 'AP'.

NOTE: Beginning with the calendar year 2007, please be aware that the United States Daylight saving time period begins on the second Sunday in March, and ends on the first Sunday in November. Refer to the "Changing Timezone Properties" section in the "Configuring RoamAbout Switch System and Administrative Parameters" chapter of the *RoamAbout Switch Manager Interface Reference* document for detailed setup instructions.

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Release	7.0.7.3	Customer Maintenance	January 2009
Previous Release	7.0.5.6	Customer Maintenance	October 2008
Previous Release	7.0.4.3	Customer Maintenance	August, 2008
Previous Release	7.0.3.7	Customer Maintenance	June, 2008
Previous Release	6.0.7.2	Customer Maintenance	April, 2008
Previous Release	6.0.6.1	Customer Maintenance	March, 2008
Previous Release	6.0.5.1	Customer, added RBT-8500 support	December 2007
Previous Release	6.0.4.4	Customer	October 2007
Previous Release	6.0.4.2	Customer, added TRPZ-MP-620 support	September 2007
Previous Release	5.0.12.2	Customer, added TRPZ-MP-422 support. Includes DFS2 Support for North American Models: RBT-1002 Rev 6A (AP ID: AP1002C), RBT-4102 Rev 6A (AP ID: AP4102C), RBT-1602 Rev 6A (AP ID: AP1602C)	June 2007
Previous Release	5.0.11.4	Customer	April 2007
Previous Release	5.0.10.3	Customer – Patch	March 2007
Previous Release	5.0.9.3	Customer	February 2007
Previous Release	5.0.9.2	Customer, added RBT-8210 support	January 2007
Previous Release	5.0.6.1	Customer, added TRPZ-MXR-2 support	December 2006
Previous Release	4.2.5.1	Customer, added RBT-8110 and	October 2006

Status	Version No.	Type	Release Date
		TRPZ-MP-620 support	
Previous Version	4.1.11.0	Customer	June 2006
Previous Version	4.1.5.0	Customer	April 2006
Previous Version	4.1.4.0	Customer, added RBT-8200 support	February 2006
Previous Version	4.0.21.0	Customer	January 2006
Previous Version	4.0.20.0	Customer	December 2005
Previous Version	4.0.18.0	Customer	November 2005
Previous Version	4.0.16.0	Customer, added RBT-8400 support	September 2005
Previous Version	4.0.7.0	Customer	August 2005
Previous Version	4.0.4.0	Customer, added RBT-8100 support	July 2005

NOTE: For firmware release 5.0.12.2, please read the TechTip on page 22for the channel availability information.

HARDWARE COMPATIBILITY:

Switches:

- RBT-8100, RBT-8110, RBT-8200, RBT-8210, RBT-8400, RBT-8500, and TRPZ-MXR-2.

Access Points:

- See the Supported Access Point Table on page 1 for detailed information for version 7.0.7.3

NETWORK MANAGEMENT SOFTWARE SUPPORT:

NMS Platform	Version No.	Module No.
RoamAbout Switch Manager 50 Access Point User License	7.0.7.3	RBT-NMS-50
RoamAbout Switch Manager 200 Access Point User License	7.0.7.3	RBT-NMS-200
RoamAbout Switch Manager unlimited User License	7.0.7.3	RBT-NMS-UNL
RoamAbout RF Planning Tool	7.0.7.3	RBT-RFPLAN
SmartPass Guest Access	7.0.7.3	TRPZ-SP TRPZ-SP-ENT

RBT-8400 Platform	Version No.	Module No.
RBT-8400 40 Additional Access Point Upgrade License	7.0.7.3	RBT-8400-40
RBT-8400 80 Additional Access Point Upgrade License	7.0.7.3	RBT-8400-80

RBT-82x0 Platform	Version No.	Module No.
RBT-82x0 24 Additional Access Point Upgrade License	7.0.7.3	RBT-8200-24
RBT-82x0 48 Additional Access Point Upgrade License	7.0.7.3	RBT-8200-48

RBT-8500 Platform	Version No.	Module No.
RBT-8500 32 Additional Access Point Upgrade License	7.0.7.3	RBT-8500-32

SUPPORTED FUNCTIONALITY:

Please refer to the following documents available at http://secure.enterasys.com/support/manuals for more details on new 7.0 enhancements and overall functionality:

RoamAbout Switch Manager 7.0 Configuration Guide	RoamAbout Mobility System Software 7.0 Command Reference Guide
RoamAbout Switch Manager 7.0 Management Guide	RoamAbout Mobility System Software 7.0 Feature Guide
RoamAbout Switch Manager 7.0 Feature Guide	RoamAbout Mobility System Software 7.0 Configuration Guide
RoamAbout Switch Manager 7.0 Planning Guide	RoamAbout Mobility System Software 7.0 Quick Start Guide
RoamAbout Switch Manager 7.0 Quick Start Guide	

New Product Features in Release 7.0	
Enterasys Virtual Controller Cluster	TRPZ-MP-432 to support 802.11n
Layer 2 ACL Enhancements	Snoop Filter Enhancements
Bandwidth Management by User and SSID	Dynamic RADIUS Extensions
MAC User Range Authentication	MAC Authentication Request Format
Additional User AAA Attributes for User Name and Simultaneous Logins	Group-based Authentication and Authorization
Location Policy Enhancements	RADIUS Ping
RF Enhancements	Mesh Enhancements

NOTES:

- Local switching is only available in RAS firmware version 6.0 and higher.
- Restricting Layer 2 forwarding for a VLAN is not supported if the VLAN is configured for local switching.
- The DHCP restrict feature is not supported for locally switched clients.
- Web Portal is not supported for locally switched clients.
- IGMP snooping is not supported with local switching.
- Locally Switched AP's can support a total of 25 ACL rules, including both inbound and outbound ACLs.
- For Wireless bridging, here are some best practice guidelines:
  - When connecting a Mesh Portal to the network, use only ethernet port 1 on the AP.
  - Because all AP CPU cycles are devoted to bridging, make other arrangements for service coverage in the bridge area as the endpoints cannot provide other wireless services.
  - A single radio must be devoted to maintaining the bridge.

Existing Product Features	
RF Load Balancing	Mesh Services
Local Switching – also known as **Direct Path Forwarding**	Wireless Bridging
Enforceable Beacon Data Rate Control	Logout for Web Authentication
RAS Seed Redundancy	Password Management
WebView 2 – updated Web interface	RBT-RBT security (also called RAS-RAS security)
AirDefense software support on APs	AeroScout RFID tag support
Persistent VLAN assignment for roaming clients	Simplified Web-Portal and last-resort configuration
RF Auto-Tuning enhancements	Unscheduled Automatic Powersave Delivery (U-APSD) support
Local software images on AP's	DHCP server enhancements
RADIUS accounting enhancements	Support for special characters in SNMP community names
Increased life span of new self-signed certificates	Web Interface to RASM services
Web-Start Client	Static IP configuration for Aps
Sygate On-Demand Agent (SODA)	Broadcast settings per Wireless profile
Configurable data rate settings for clients	Session Based Call Admission Control
Static Class of Service	User Session Timers per SSID
Network Planning and Site Survey	Management services
SSID (Wireless Service)	Radio and Service profiling
Load Sharing	802.1Q VLANs
Spanning Tree – PVST	AAA/802.1X
ACLs	IP services
RF detection	Rogue detection
Countermeasures	Client and AP monitoring
Site policies	Reporting
Image repository and deployment	Auto-AP configuration
L2 traffic restriction	Default AAA attributes for each SSID
On-demand countermeasures	Network Domains
Configurable timeout for the RoamAbout Switch CLI sessions	Configurable CoS to QoS mappings

INSTALLATION AND CONFIGURATION NOTES:

In general, the RoamAbout Wireless Switch RBT-8xx0 has been, or is being, shipped to you with a previous firmware version. Please refer to the appropriate *RBT-8xx0 Quick Start* or the *RBT-8xx0 Installation Guide* for hardware installation information. Please refer to the next section, *Upgrading the RBT-8xx0 Switches*, for upgrading information and procedures.

UPGRADING THE RBT-8XX0 SWITCHES FROM PREVIOUS 4.0.X VERSIONS:

Minimum RAS Requirements for Upgrade

Product	Minimum RAS version required	Recommended Upgrade Path
RBT-8100	4.0.4.0	6.0.7.2 → 7.0.7.x
RBT-8200	4.1.4.0	6.0.7.2 → 7.0.7.x
RBT-8110, RBT-8210	4.2.5.1	6.0.7.2 → 7.0.7.x
RBT-8400	4.0.16.0	6.0.7.2 → 7.0.7.x
RBT-8500	6.0.5.1	6.0.7.2 → 7.0.7.x

Note: You must upgrade to RAS Version 5.0 or later before upgrading to RAS Version 7.0.

Preparing the RAS for the Upgrade

Note: The following upgrade procedures refer to all RBT-8xx0 switches.

Caution!

Save the configuration, and then create a backup of your RAS files before you upgrade the switch. Enterasys Networks recommends that you make a backup of the switch, before you install the upgrade. If an error occurs during the upgrade, you can restore your switch to its previous state. If you later decide to downgrade the switch, commands with newer syntax in future RAS versions may not be converted correctly.

1. Use the following command to save the configuration. Unsaved changes will be lost during the upgrade procedure:

   ```
   RBT-8xx0# save config [filename]
   ```

2. The following command should be used to back up the switch's files:

   ```
   RBT-8xx0# backup system [tftp://ip-addr/]filename [all | critical]
   ```

3. To restore a switch that has been backed up, use the following command:

   ```
   RBT-8xx0# restore system [tftp://ip-addr/]filename [all | critical] [force]
   ```

The "Upgrade Scenario" listed below shows an example use of the backup command. For more information about these commands, see the "Backing Up and Restoring the System" section in the "Managing System Files" chapter of the *RoamAbout Mobility System Software Configuration Guide*.

Note: If you have made configuration changes but have not saved the changes, use the **save config** command to save the changes, before you back up the switch.

If the RAS is running an earlier version of firmware, use the **copy tftp** command to copy files from the switch onto a TFTP server.

Upgrading an Individual Switch Using the CLI:

1. Save the configuration, using the **save configuration** command.

2. Back up the switch, using the **backup system** command.

3. Copy the new system image onto a TFTP server.

   For example, login to http://www.enterasys.com/download/ using a web browser on your TFTP server and download the image onto the server.

4. Copy the new system image file from the TFTP server into a boot partition in the switch's nonvolatile storage. You can copy the image file only into the boot partition that was not used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.

5. Set the boot partition to the one with the upgrade image for the next restart.

   a. To verify that the new image file is installed, type show boot.

6. Reboot the software.

   a. To restart a RAS and reboot the software, type the following command:

      ```
      RBT-8xx0# reset system [force]
      ```

   After resetting the RAS, the switch boots using the new image. The RAS also sends the AP version of the new boot image to the configured APs and restarts the APs. After an AP restarts, it checks the version of the new AP boot image to make sure the boot image is newer than the boot image currently installed on the AP. If the boot image is newer, the AP completes installation of its new boot image by copying the boot image into the AP's flash memory, which takes about 30 seconds, then restarts again. The upgrade of the AP is complete after the second restart.

Upgrade Scenario:

To upgrade an RBT-8xx0 switch from one RAS version to another, type commands such as the following.

Note: This upgrade scenario uses the firmware image file 6.0.7.2 to show the download features. Please follow these procedures for any of the 4.0.x, 4.1.x, 4.2.x, and 5.0.x firmware images.

Note: This example copies the image file into boot partition 1. On your switch, copy the image file into the boot partition not used for the last restart. For example, if the switch booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the show boot command.

```
RBT-8200# save config success: configuration saved.
RBT-8200# backup system tftp:/[ip-addr]/sysa_bak success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
RBT-8200# copy tftp://[ip-addr]/R2060701.REL boot1:R2060701.REL success: received 11257345 bytes in 16.230 seconds [693613 bytes/sec]
RBT-8200# set boot partition boot1 success: Boot partition set to boot1.

RBT-8200# show boot
Configured boot version:        6.0.7.2.0
Configured boot image:          boot1: R2060701.rel
Configured boot configuration:  file:configuration
Backup boot configuration:      file:backup
Booted version:                 6.0.6.1.0
Booted image:                   boot0:R2060601.REL
Booted configuration:           file:configuration
Product model:                  RBT-8200
```

Upgrading an Individual Switch Using the RoamAbout Switch Manager (RASM)

Please refer to the chapter “Managing with RoamAbout Switch Manager”, section “Distributing System Images” in the *RoamAbout Switch Manager Management Guide* when upgrading the RBT-8xx0 switch to the released version.

SYSTEM PARAMETER SUPPORT:

RoamAbout System Parameters:

Parameter:	Supported Value:
RASs in a single Network Domain	500
RASs in a single Mobility Domain	32
Roaming VLANs per RAS	300 Does not include local statically configured VLANs
VLANs per Mobility Domain	400 This number consists of 300 roaming VLANs plus 100 local statically configured VLANs
APs per RAS	RBT-81x0: 60 configured, 24 active RBT-82x0: 180 configured, 72 active RBT-8400: 300 configured, 120 active RBT-8500: 320 configured, 128 active
SSIDs per radio	8
Minimum link speed within a Mobility Domain	128 Kbps

Network Parameters:

Parameter:	Supported Value:
Forwarding database entries	RBT-81x0: 8192 RBT-82x0: 8192 RBT-8400: 16383 RBT-8500: 8192
Statically configured VLANs	128
Virtual ports (sum of all statically configured VLAN physical port memberships)	256
Spanning trees (STP/PVST+ instances)	64
ACLs and Location Policies	ACEs per switch RBT-81x0: 700 RBT-82x0: 700 RBT-8400: 2308 RBT-8500: 2308 ACEs per ACL: RBT-81x0: 25 RBT-82x0: 25 RBT-8400: 267 RBT-8500: 267 Locations Policies per switch: All models: 1 The Location Policy can have up to 150 rules. ACL rules (ACEs) with Local Switching (Direct Path Forwarding) enabled: 25
IGMP Streams	500 Note: Replications of a stream on multiple VLANs count as separate streams on each VLAN.

Management Parameters:

Parameter:	**Supported Value:**
Maximum instances of the RoamAbout Software Management system simultaneously managing a network	3
Telnet management sessions	RBT-81x0: 8 RBT-82x0: 8 RBT-8400: 8 RBT-8500: 8 **Note:** The maximum combined number of management sessions for Telnet and SSH together is 8 for the RBT-8400, RBT-81x0, and the RBT-82x0.
SSHv2 management sessions	RBT-81x0: 8 RBT-82x0: 8 RBT-8400: 8 RBT-8500: 8
Telnet client sessions (client for remote login)	RBT-81x0: 8 RBT-82x0: 8 RBT-8400: 8 RBT-8500: 8
NTP servers	3
SNMP trap receivers	8
Syslog servers	4
RADIUS servers	100 configured on the switch 10 in a server group 4 server group in a AAA rule

Client and Session Parameters:

Parameter:	**Supported Value:**
Authenticated and associated clients per radio	100 Clients who are authenticated but not yet associated are included in the total
Active clients per radio	50 Total number of active clients simultaneously sending or receiving data
Active AAA sessions (clients trying to establish active connections) per RAS switch	RBT-81x0: 600 RBT-82x0: 1800 RBT-8400: 2500 RBT-8500: 3200
AAA users configured in local user database	RBT-81x0: 999 RBT-82x0: 999 RBT-8400: 999 RBT-8500: 999

FIRMWARE CHANGES AND ENHANCEMENTS:

Firmware Release 7.0.7.3:
Resolved an issue where static WEP keys did not work for some service profiles.
Resolved an SNMP error that caused an AP to become unresponsive.
Resolved an issue where the RBT-8500 became unresponsive on the network.
Resolved an issue where a large number of user sessions caused the Web portal login page to become inaccessible.
Resolved an issue where merging configurations between the primary and secondary seed caused the RASs to become unresponsive.
Resolved an issue where using a question mark symbol in a Web AAA page URL caused the page to not display properly.
Resolved an issue where the TCP connection to the RAS did not close immediately after sending a 403 error in response to a request from a Skype client.
Resolved an issue where a corrupted cluster configuration update caused the RAS to become unresponsive.
Resolved an issue where configuring multiple user groups and using local authentication for web logins caused the RAS to become unresponsive.
Resolved an issue where MSS did not report the maximum transmit power on any particular channel as a proxy for the maximum power allowed by the regulatory domain.
Resolved an issue where a large number of location policies caused the cluster configuration to be unresponsive.
Resolved an issue where the show network verbose command displayed the incorrect output in the CLI.
Resolved an issue where upgrading to a later version of MSS caused the RAS to become unresponsive.
Resolved an issue where a corrupted control packet caused the AP to become unresponsive.
Resolved an issue where an invalid IGMP message caused the RAS to become unresponsive.
Resolved a problem where some 802.11n wireless adapters experienced packet loss on wireless services with the SVP enabled. Existed only on the TRPZ-MP-432.
Resolved a TCP buffer issue that caused a RAS within a Mobility Domain to crash.
Resolved a corrupt control packet issue causing APs to become unresponsive and reset.
Resolved an issue that, when using MacOS, an unsupported protocol option would cause SSH admin connections to fail.
Resolved an issue where Auto-tune’s lower boundary was not implemented for AP power tuning.
Resolved an issue where an invalid AP configuration caused the RAS to become unresponsive.
Resolved an issue where a large number of EAP offload sessions caused the RAS to crash.
Resolved an issue where, in certain configurations, the RAS incorrectly reports channel configuration.

Firmware Release 7.0.5.6:
Resolved an error message: “network: radio_decode_data: read A-MSDU subframe snap header failed” occurred on the network.
Resolved an issue that caused MIC errors on the network when configuring WPA TKIP.
Resolved an RBT-8500 memory corruption at cfg_memory.c error message that caused network problems.
Resolved an issue where the RBT-8xxx sent too many access requests to the RADIUS server after configuring RADIUS to authenticate users with EAP-TLS, or EAP-PEAP.
Resolved an issue where SSIDs using "#" as part of the name were not accepted in the configuration.
Resolved an issue with Internet Explorer and WebView where the date format was displayed incorrectly.
Resolved an issue reloading a configuration with cluster mode enabled prevented RASM from determining the active seed.
Resolved an issue with clients that could not re-associate without first authenticating on the network.
CAPWAP data plane UDP port changed from 5001 to 5247.
Resolved an issue when using telnet over a WAN link adversely affected the telnet session.

Firmware Release 7.0.5.6:
Resolved an issue when using the active-scan feature triggered packet loss on legacy MPs/ RASs with older Intel wireless adaptors.

Firmware Release 7.0.4.3:
Resolved an issue where reloading a configuration with cluster mode enabled prevented RASM from determining the active seed.
CAPWAP data plane UDP port changed from 5001 to 5247.
Resolved an issue where the active-scan feature triggered packet loss on legacy APs with older Intel wireless adaptors.

Firmware Release 7.0.3.7:
Support for TRPZ-MP-432 802.11N access point
Resolved a reporting issue with RF Monitoring and port monitor.
Resolved an issue with large fragmented packets across WAN.

Firmware Release 6.0.7.2:
Added support for the RBT-4102 internal and external antennas.
Resolved an issue in RAS firmware that caused RASM to report an Empty or Missing device and Protocol error 503.
Resolved an issue where certain client types would not connect to an 802.1X network using WPA with AES cipher.
Resolved an issue where user sessions with end-date attributes set to more than 20 days in the future (relative to controller time/date) cause system crashes with a core dump.
Resolved an issue on the platform controllers, RBT-8400, where all client sessions would drop due to the application of additional user-based ACL's once the platform scalability limit of ACL's has been reached.
Resolved an issue where the RAS would crash due to a packet leak issue.
Resolved an issue with the command "show ap global". When the command was run on a Mobility Domain with access points configured in a redundant mode, only the APs configured for High Bias on that RAS appeared.

Firmware Release 6.0.6.1:
Resolved an issue where the filter-ID was only working with colons not semicolons.
Resolved an issue where the ETS logo in Webview screens showed the outdated image.
Resolved an issue where an IP Checksum Error caused slow network performance.
Resolved an issue where the RF fingerprint checking resulted in AP Spoofing alarms.
Resolved a DAP (AP) power auto-tuning issue where DAPs (or AP's) changed power frequently and incorrectly.
Resolved an issue where the user glob for accounting could not be set to ** in the CLI.
Resolved an issue where GuestPass users using the Web portal page timed out before reaching the default 802.1X time.
Resolved an issue where the Access Point strips the VLAN header from a tagged packet before the Tunnel encapsulation from the AP to the RAS. This occurs with Direct Path Forwarding (Local Switching) enabled on the Access Point.
Resolved an issue where the installation of a CA certificate was not recognized by the RAS if the certificate chain were included in the CA certificate file.
Resolved an issue where the RBT-4102-EU AP would crash after receiving 6 or more DNS requests.
Resolved an issue where client roaming was slow or failed altogether under heavy load on the Access Point. The TXOP limit is sometimes included in AC Voice, and sometimes it does not appear (but the length of the WMM element is the same). In addition, some management frames are two bytes smaller than what they specify because the radio driver appears to be stripping 2 bytes off management frames in certain situations.

Firmware Release 6.0.5.1:
The number of packets in the DNS packet queue increased from 3 to 8.

Firmware Release 6.0.5.1:
The 6.0.5.1 release now supports 25 ACL rules (ACEs) per ACL, total of inbound and outbound, to be mapped to the user if the AP has Direct Path Forwarding (Local Switching) enabled. There can be more than one ACL, with 25 ACEs, applied to multiple users on the AP. If an ACL with 26 or more rules is mapped to the user with Local Switching enabled, the users in the network will not connect or authenticate to that wireless network. Enterasys Networks recommends creating separate ACL profiles to be used for those users who are authenticated into the Local Switching VLAN profile.
Resolved an issue with the Web Authentication page and login slowness due to the memory buffer for non-parsable http requests not being freed.
Resolved a memory leak issue in the TCP machine that caused Netsys crashes. The memory was not freed in cases where the client attempts to close the tcp connection from its end but we still have some data to send out.
Resolved an issue where certain wireless IP phones would not connect to the AP1002, RBT3K-AG, or RBT-4102.
Resolved an issue where Radius calling-station-id not sent by the Web-portal functionality.
Resolved an issue where an NMAP scan would cause the web portal page to no longer function.
Resolved an issue where a WebView error was seen for the browser URL reference icon.
Resolved an issue where ACL rules were not applied to a Locally switched user.
Resolved an issue where certain fdb errors were seen on a Mesh AP after it was reset.
Resolved an issue when the login WebAAA page displayed a partial logo or title header.
Resolved an issue where a Bonded Authenticated user would not get an IP address using the TKIP cipher.
Resolved an open endian issue where an ICMP ACL rule (ACE), with either the source or destination IP address fields and masks configured, will not get applied to an authenticated user with Direct Path Forwarding (Local Switching) enabled.
Resolved an issue where the ACL Mapping with Local Switching fails after adding the 17th ACL rule.

Firmware Release 6.0.4.4:
Resolved an issue where a bit on the non-mesh supported Access Points could be randomly set, causing the APs to reset several times.
Resolved an issue where an external antenna attached to the TRPZ-MP-422 Access Point was not transmitting the configured power.
Resolved an issue for the RBT-8400 where system generated core crash files were truncated and unreadable.

Firmware Release 6.0.4.2:
Added support for the TRPZ-MP-620 Outdoor Access Point. Direct Path Forwarding (Local Switching), Mesh Services, and Wireless Bridging are only supported on the TRPZ-MP-620 and TRPX-MP-422 Access Points.
The RBT-8400 image is smaller than previous releases due to a shared library format introduced in the 6.0 firmware. Statically linked executables, which called to individual library functions, were replaced with run-time calls, reducing the total number of individual library routines to be opened, and reducing the overall size of the firmware required to operate the network switch. This format also increases the amount of memory available for data transfer and table maintenance.
Resolved the issue where the Static IP configuration and deployment for the AP4102 and AP3000 did not remain persistent with the AP upon reboot.
Resolved the erroneous message error printed to the CLI when the RBT-8400 reboots with 5.0.12.2: Bootloader upgrade 5.0.x to 5.0.x needed. (x could be any number) cp: /boot0/bload: No space left on device
Resolved an issue where the TRPZ-MP-422 Access Point image does not load with the 6.0.x code.
Resolved an issue where the configured APs in a network plan would crash upon RAS firmware upgrade due to a DNS update entry on the RAS.
Resolved an issue where the Radius CLASS attribute was not sent with stop packets.
Resolved an issue where the RAS spoofed a DNS reply with a 169.254.x.x if the DNS server took more than 3 seconds to respond. Certain Linux and Vista users will drop this packet causing everything to fail
Resolved an issue where the configured APs would crash with various exception messages, including TLB data miss and sigtrap.

Firmware Release 6.0.4.2:
Resolved an issue where an expired password could be used to log into the system.
Resolved an issue where the APs may reset if the traffic load to the RAS host IP address exceeds 200Mb/s.
Resolved an issue where the configured AP name is not shown in the SNMP trap.
Resolved an issue where IP addresses were transposed in MIB queries that returned IP address information.

Firmware Release 5.0.12.2:
Added support for the TRPZ-MP-422 Access Point.
Added support for the following DFS2 compliant North American model Access Points: RBT-1002 Rev 6A (AP ID: AP1002C), RBT-4102 Rev 6A (AP ID: AP4102C), RBT-1602 Rev 6A (AP ID: AP1602C). Please see the DFS2 Tech Tip on page 22 for further information.
Resolved an issue where the RAS can lock-up when a Nessus scan is deployed against the switch.
Resolved an issue where the RAS sends the NAS port attribute four (4) times in a RADIUS request.
Resolved an issue where the RAS tunnel functionality would fail to report the status of other RB switch members in the network domain.
Resolved an issue where the VLAN member information was not added to the RAS configuration when using the WebView Quickstart for initial configuration.
Resolved a WebView issue where a second VLAN's interface IP information would display an error if the bit mask were set for less than 8 bits.

Firmware Release 5.0.11.4:
Resolved a DAP crash issue where a buffer in the Access Point is being written past the end with too much data and corrupting the header of the following buffer.
Resolved an issue where the RBT-8400 CPU utilization increases due to a DHCP request packet looping issue with the port- trunk functionality.
Resolved an ASSERT and exception DAP crash due to a corrupted link header when the DAP is rebooting. This issue occurred when a packet entered the AP through the Ethernet MAC, and the Access Point stored this packet in memory spot in which the operational code needed zeroed out.
Resolved an issue where the RBT-1002 Ethernet port would transition to half-duplex under heavy traffic load (approximately 25 Mbps throughput).
Resolved an issue where the WebAAA login page would not resolve due to a certificate failure on a client using the Vista OS and Microsoft Internet Explorer version 7. The workaround is for the client to open the Internet Explorer browser as "Administrator" and accept the WebAAA certificate.
Resolved an issue where a client using the Vista OS and Microsoft IE 7 failed to get the WebAAA login page when the Common Name in the RAS Web certificate equals '*.<domain>.com'.
Resolved an issue where the radio information was not displayed after issuing the "show sessions" command.
Resolved an issue where the RBT-8400 locked-up due to a processor losing entries in the FDB, and over time, the processor would lose the CPU entry, causing the lock-up.
Resolved an issue where DAP's were crashing due to Filter Database issues and causing ASSERT errors on the RAS.
Resolved an issue where the message "radar is no longer detected" would continuously scroll across a console screen when the DAPs auto-tuned the channel from a DFS channel to a non-DFS channel.
Resolved an issue when the RBT-8400 would show 'Username: IP=127.0.0.1' after a switch reboot.
Resolved an issue where the auto-configuration setting changes for the B/G radio via WebView were not shown in the active RAS configuration.
Resolved an issue when the DAP reboots with an ASSERT error when WMM-powersave is enabled.
Functionality description for an open issue where the DAP system uptime is changing, but the DAP has not rebooted. DAP's that change from a low bias switch to a high bias switch are expected to reset without showing a system log error.
Resolved an issue where the DAP would crash when countermeasures attempted to use an 11a radio to attack a rogue on an 11b channel.
Resolved an issue where AP_Handshakes errors continuously scrolled across the console connection.
Resolved an issue with a DAP Exception when the DAP tried to tune 11a radio to an 11bg channel.

Firmware Release 5.0.11.4:
When configuring the Web portal and saving the default login page, remove everything between the quotes in the Action value of the form tag in the HTML code.
Resolved an issue where the Access Point buffers were filling up with Rogue Detection messages.
Resolved an issue when a wireless client was previously connected to an SSID (WebAAA, last-resort), then switched to a new bonded auth SSID, the machine auth phase was skipped.
Resolved an issue when rebooting the RAS via the CLI command “reset system” does not generate a 'warm start' SNMP. Instead, a 'cold start' trap is sent.
Resolved an issue when clients who authenticated to a switch with a low bias DAP moved to the high bias switch when the switch became available.
Resolved an issue where using the same port for SSH and Telnet access caused the RAS to reboot.
Resolved an issue where setting ports as a port group, then changing one port to wired-auth type, caused the RAS to become unresponsive.
When downgrading from 5.0 to 4.1 (and earlier releases), changes may be required in the 4.1 configuration if the 5.0 configuration had a service profile with last-resort or web-portal access. Specifically, an authentication access rule must be added for last-resort users and the correct VLAN (and other attributes) may need to be set for the last-resort-<ssid>, web-portal-<ssid> special users. Earlier 4.2 versions contain a script that sets the special user attributes and the last-resort access rule on downgrade from 5.0. It is highly recommended in any case to back up the 4.x configuration before upgrading to 5.0.
Resolved an issue where using the “monitor port counter receive-errors” command displays statistics in wrong order.

Firmware Release 5.0.10.3:
Resolved an issue with the RBT-4102 not coming back online if connected to a non-PoE switch and power or reset cycle was initiated to on host RBT-8xxx controller switch.
Based upon the previous resolution, the thin DAP boot-loader number has been incremented, so the new bootloader code will be automatically downloaded to the DAP.
Resolved an issue where the Client MAC address was not flushed from the FDB after a DAP disconnect.
Resolved an issue where corrupted TAPA packets from configured DAPs were causing the RAS to core crash.
Resolved an issue where a DAP is broadcasting a DHCP request to every IP address renewal. If two DHCP servers are on the same segment this could cause a different DHCP server to send a DHCP response. When this happens it will reboot the DAP even if it already received a DHCP acknowledgement from the correct DHCP server (which was used previously).
Resolved an issue where the RAS generated excessive ROGUE_AP_ALERT:rfslave_handle_packet messages, possibly affecting the DAPs to run countermeasures.
Resolved an issue with multiple core crashes on RASs with “ASSERT” errors and DAP loss due to increased traffic spikes in the network.

Firmware Release 5.0.9.3:
Resolved an issue for a performance problem with one of the encryption methods used in the supported access points. Due to a change to the Atheros radio driver code, the WPA/TKIP protocol was executed in software instead of in hardware. This led to a reduction in throughput of approximately 33% for that encryption type. This problem also brought with it a chance of CPU over utilization that could lead to the access point rebooting while under heavy WPA/TKIP traffic load.
Resolved an issue where connection loss occurred between the Intel 3945 Internal Wireless NIC and the non-broadcasting SSID from the RoamAbout Switch system.
Resolved an issue where the RAS reported a “DAP: Recv Seq Cntr Failure” error message from clients using WPA-TKIP authentication, causing some clients to lose wireless connections to the network.

Firmware Release 5.0.9.2:
Added support for the RBT-8210. This RAS, along with the current RBT-8200, will be known as the RBT-82x0 family.
Resolved an issue where DAPs would reset with an ASSERT error, due to traffic spikes in the network.
Resolved an issue where the RBT-1002-EU would crash with an ASSERT error after an image download.
Resolved an issue where a custom web page was not displayed after the client successfully authenticated against the Access Point.
Resolved an issue where blank DNS and IP Router Fields in WebView resulted in a WebView IP Services error.
Resolved an issue where VLAN ports could not be selected in WebView.
Resolved an issue where the RAS would core dump after querying the rbtwsSysDataObjects MIB branch.
Resolved an issue where the RBT-4102-EU and the RBT-1002-EU were not supported in the country code Hong Kong.
Resolved an issue when the RAS would report an SSL error or System communication errors after generating a certificate signing request via WebView.
Resolved an issue when the current RAS configuration was not cleared after using the Quickstart feature via WebView.
Resolved an issue where clients using a Macbook Pro could not connect to the RAS.
Resolved an issue where the Web portal login screen would not propagate to the client after a successful authentication
Resolved an issue where one RAS configured for DAP load balancing and redundancy with a second RAS continually reset after losing contact with configured DAPs.
Resolved an issue where the sixth (or more) DAP would crash using the Quickstart feature.
Resolved an issue when the switch received an ARP packet with a source address of all zero's, it would cause a tunnel crash.

Firmware Release 5.0.6.1:
Added support for the TRPZ-MXR-2 switch.
Resolved an issue where the DAP Operational Power was showing a N/A value for the country code Argentina.
Resolved an issue where an error message reading "EAP_STORE_ERR" would appear on the CLI console of the RBT-8110.
Resolved an issue where extra characters were added to the banner MOTD after a firmware upgrade on the RAS.
Fixed an issue where a possible unicast flood condition could occur with redundant RBT-8400 switches.

Firmware Release 4.2.5.1:
Static IP configuration for DAPs – These settings are only available through the CLI interface on the switch. The user now can set a static IP address, RAS name or RAS address, and VLAN on the Access Points. These settings are persistent on the RBT-1602 and the RBT-1002 Access Points only for the current 4.2.5.1 firmware.
Resolved an issue where the RBT-4102 and the RBT3K-AG would not boot due to an RSA fingerprint match failure.
Resolved an issue with the WPA sequence number used to help sync up the per-packet keys between the Intel 3945 A/B/G chipsets and any Access Point in the RAS system. Clients would authenticate successfully against the RADIUS server, but not have any connectivity to the network.
Resolved an issue where extra carriage returns in the banner MOTD would cause the RAS to fail an upgrade and constantly reboot.
Resolved an issue where the RBT-8400 would core crash and lose part of the active configuration upon upgrade.
Resolved an issue where the RAS core crashed after cutting and pasting a "set port group" CLI command.
Resolved an issue where the Quickstart configuration helper was automatically creating an admin password.
Fixed the length of the CLI entry for the mobility domain name from 16 to 32 characters.
Resolved a CLI command issue where the CLI would lock up after rapidly entering a "show load" command (3-5 times within 5-10 seconds).

Firmware Release 4.2.5.1:
Resolved an issue where “set dap” commands would not return a “succeed: changes accepted” notification.
Resolved an issue where a switch reset with multiple core files after a system upgrade. Core resets were attributed to the enabling of rogue detection in the fabric.

Firmware Release 4.1.11.0:
Added support for the RBT-4102 North American Access Point.
Resolved an issue where RBT-1602s would reset every 18 hours and report a fingerprint mismatch error.
Resolved an issue where the RBT-1602 would report a power level outside its regulatory limits, causing a configuration mismatch.
Resolved an issue where the RBT-1002 DAPs would not boot up due to a switch and homologation configuration download timing issue (switch DAP configuration would get pushed down before the homologation information had finished processing).
Added support for the following countries in the RBT-4102-EU and RBT-1002-EU AP models: (NOTE: Check the regulatory requirements or local Enterasys personnel to insure that the product is certified in your country.)

AU	AUSTRALIA	VN	VIETNAM
CN	CHINA	EG	EGYPT
IN	INDIA	KW	KUWAIT
JP	JAPAN (W52/W53)	IL	ISRAEL
KR	KOREA, REPUBLIC OF	SA	SAUDI ARABIA
MY	MALAYSIA	AE	UNITED ARAB EMIRATES
NZ	NEW ZEALAND	AR	ARGENTINA
PH	PHILIPPINES	BR	BRAZIL
SG	SINGAPORE	VE	VENEZUELA
TW	TAIWAN	ZA	SOUTH AFRICA
TH	THAILAND		

Resolved an issue where WPA2 clients roaming through the mobility domain would resend their RADIUS authentication information, forcing a re-association.
Resolved an issue where the RBT-8100 would core dump after processing a serial debug command.
Resolved an issue where the RBT-8400 eeprom (nvram) settings were corrupted after code upgrade.
Note: Refer to the Tech Tip on page 22 for important information about configuring antenna types for an RBT-1602 Access Point.

Firmware Release 4.1.5.0:
The AP1102 and AP1102-EU names have been changed to RBT-4102 and RBT-4102-EU. If you are installing this code onto pre-existing RBT-4102-EU models (with 4.1.4.0 firmware), then please refer to the RoamAbout Switch Manager (RASM) 4.1.5 Release Notes for complete instructions to upgrade your AP correctly.
Resolved an issue where the DAPs were not responding to the bias settings correctly for AP redundancy.

Firmware Release 4.1.4.0:
Added support for the RBT-8200 RAS, and the RBT-1002-EU and RBT-4102-EU Access Points.
Resolved an issue where the RBT-8100 would crash after a dot1x authentication using MSCHAPv2.
Resolved an open issue dealing with the configuration and operation of Third-Party APs.
Resolved an issue where the Called-Station-ID RADIUS attribute was not returning from the RoamAbout Switches.
Resolved an issue where the RBT-8100 Ethernet ports could be enabled for PoE (ETS only supports Distributed Access Points, and while the directly connected access point configuration will work, it is not a supported configuration).
Resolved a tunnel:core dump issue which occurred after issuing a reset DAP command.
Resolved a DNS memory issue when the DNS functionality was disabled and the RBT-8100 auto-configuration was enabled.

Firmware Release 4.0.21.0:
Resolved an issue where ACLs were not properly assigned to users due to the incorrect parsing of the Enterasys filter ID string (Enterasys:version=1:policy=<policy name>) returned from a RADIUS server.
The default MAC authentication RADIUS password has been changed from ‘nopassword’ to ‘NOPASSWORD’.

Firmware Release 4.0.20.0:
Added support for the RBT-1602 Access Point.
Increased the limit of local mac authenticated users from 75 to 2400 (this fix was originally listed in the 4.0.18.0 Firmware Release section, but the implementation did not occur until this 4.0.20.0 release).
Resolved the issue where a WebAAA user would not be redirected to a web page if the proxy setting were enabled.

Firmware Release 4.0.18.0:
MTU for Tunneled traffic was too long — Previous versions of MSS required an IP Path MTU (PMTU) of 1484 bytes for tunneled traffic, and used a non-standard implementation of IP Fragmentation to transport IP datagrams larger than that PMTU. Because of the non-standard fragmentation, tunnel IP datagrams could be dropped by devices attempting to validate packets for proper formatting. The current MSS version fixes this issue. IP Fragmentation is supported in accordance with RFC 2003. This change allows third-party devices in the communication path to validate properly fragmented tunnel IP datagrams. In addition, the maximum packet size is smaller. In the current MSS version, the PMTU requirement has been reduced to 1384 bytes, to allow devices along the communication path to encapsulate further the tunnel packets without introducing additional fragmentation.
Resolved an issue where associated clients (to clear SSID) could access WebView and changing system configurations.

Firmware Release 4.0.16.0:
Added support for the RBT-8400 RAS and the RBT-1002 Access Point.
Resolved an issue where MAC addresses would be dropped from the Filter Database without the session timing out (fdb hashing error in the database).
Resolved an issue where the RBT-8100 would have a core dump after trying to save a configuration file with a name longer than 16 characters.
Resolved an issue where a user would not get a DHCP address using WebAAA and the internal DHCP server on the RBT-8100.
Resolved the password recovery method, where the “Esc” prompt during the RBT-8100 boot-up cycle appeared too late in the boot-up cycle.
Resolved an issue where the Service Profile would only allow a 16-character name.

Firmware Release 4.0.7.0:
Resolved an issue where Distributed APs would reset across a routed network.
Resolved an issue with RBT-8100 port auto-negotiation.
Resolved an issue when an RBT-8100 would display the wrong prompt values after clearing the system configuration.

Firmware Release 4.0.4.0:
Initial Release for the RBT-8100 RAS and the RBT3K-AG Access Point in thin mode.

You should check our web site on a regular basis for updates at http://www.enterasys.com/products/wireless/.

KNOWN RESTRICTIONS AND LIMITATIONS:

Firmware Release 7.0.7.3:
802.11n adapter incompatibility with Spectralink Voice Protocol (SVP) enabled service profiles. **Description —** Some 802.11n wireless adapters may experience packet loss on wireless services with the Spectralink Voice Protocol enabled. This problem only exists when using the TRPZ-MP-432 with frame aggregation enabled. **Workaround —** When using SVP on the TRPZ-MP-432 disable frame aggregation.
The aggregate throughput exceeds the bandwidth limit of the SSID. **Description —** Per SSID max-bw is only enforced within the scope of one radio. Therefore, if you configure multiple SSIDs per radio and configure bandwidth management on the SSIDs, you can exceed the bandwidth for each SSID. **Workaround —** Configure bandwidth management on a per radio basis. The limits for service-profile max-bw and service-profile cac-session are enforced independently on each radio.
Upgrading from MSS 6.0 to MSS 7.0 changes the antenna location from Indoor to Outdoor on the AP. **Description —** If an AP is configured with the antenna location as Indoor and you upgrade the MSS version from 6.0 to 7.0, the antenna location changes to Outdoor. **Workaround —** Reconfigure the antenna with the proper location after upgrading the MSS version.
Changes to the DTD cause incompatibility with cluster configuration. **Description —** MSS Cluster Configuration relies on configuration options being consistent between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members. **Workaround —** All RASs in a cluster configuration should have the same version of MSS.
Using the quickstart command on the TRPZ-MX-2800 incorrectly sets VLAN tag ID. **Description —** When configuring the TRPZ-MX-2800 using the quickstart command, it is possible to configure an invalid VLAN tag value for the default management VLAN. **Workaround —** After completing the quickstart configuration, create a new VLAN with the correct VLAN tag.
Using the auto-ap feature does not allow load balancing on individual radios. **Description —** When using the auto-ap feature, it is not possible to set all of the AP attributes. Per AP load balancing control is not supported on auto-ap. The system global settings for load balancing applies to all auto-aps. **Workaround —** If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.
Auto-aps do not behave correctly on cluster seed when the maximum number of APs are configured. **Description —** When a cluster seed RBT-8xxx boots an auto-ap, it checks the seed configuration on the RBT-8xxx to determine if the cluster can support any additional AP's. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly. **Workaround —** Reduce the number of configured APs in the cluster configuration.
Voice handsets can be sensitive to changes on an in-service SSID. **Description —** Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information. **Workaround —** When using affected handsets, disable the Service Profile prior to making any configuration changes.
Some RAS controllers show an incorrect CPU load. **Description —** RAS controllers show an erroneous CPU load of 100% in the command line interface. This will be fixed in the next version of MSS. **Workaround —** None.

Firmware Release 7.0.5.6:
802.11n adapter incompatibility with Spectralink Voice Protocol (SVP) enabled service profiles. **Description —** Some 802.11n wireless adapters may experience packet loss on wireless services with the Spectralink Voice Protocol enabled. This problem only exists when using the TRPZ-MP-432 with frame aggregation enabled. **Workaround —** When using SVP on the TRPZ-MP-432 disable frame aggregation.
The aggregate throughput exceeds the bandwidth limit of the SSID. **Description —** Per SSID max-bw is only enforced within the scope of one radio. Therefore, if you configure multiple SSIDs per radio and configure bandwidth management on the SSIDs, you can exceed the bandwidth for each SSID. **Workaround —** Configure bandwidth management on a per radio basis. The limits for service-profile max-bw and service-profile cac-session are enforced independently on each radio.
Upgrading from MSS 6.0 to MSS 7.0 changes the antenna location from Indoor to Outdoor on the AP. **Description —** If an AP is configured with the antenna location as Indoor and you upgrade the MSS version from 6.0 to 7.0, the antenna location changes to Outdoor. **Workaround —** Reconfigure the antenna with the proper location after upgrading the MSS version.
Changes to the DTD cause incompatibility with cluster configuration. **Description —** MSS Cluster Configuration relies on configuration options being consistent between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members. **Workaround —** All RASs in a cluster configuration should have the same version of MSS.
Using the quickstart command on the TRPZ-MX-2800 incorrectly sets VLAN tag ID. **Description —** When configuring the TRPZ-MX-2800 using the quickstart command, it is possible to configure an invalid VLAN tag value for the default management VLAN. **Workaround —** After completing the quickstart configuration, create a new VLAN with the correct VLAN tag.
Using the auto-ap feature does not allow load-balancing on individual radios. **Description —** When using the auto-ap feature, it is not possible to set all of the AP attributes. Per AP load-balancing control is not supported on auto-ap. The system global settings for load-balancing applies to all auto-aps. **Workaround —** If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.
Auto-aps do not behave correctly on cluster seed when the maximum number of APs are configured. **Description —** When a cluster seed RBT-8xxx boots an auto-ap, it checks the seed configuration on the RBT-8xxx to determine if the cluster can support any additional AP's. If the system is already configured with the maximum number of AP's allowed, new auto-aps do not operate correctly. **Workaround —** Reduce the number of configured APs in the cluster configuration.
Voice handsets can be sensitive to changes on an in-service SSID. **Description —** Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information. **Workaround —** When using affected handsets, disable the Service Profile prior to making any configuration changes.

Firmware Release 7.0.4.3:
Changes to the DTD cause incompatibility with cluster configuration. **Description —** RoamAbout MSS Cluster Configuration relies on configuration options being consistent Between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members. **Workaround —** All RASs in a cluster configuration should have the same version of RoamAbout MSS.

Firmware Release 7.0.4.3:
Using the auto-ap feature does not allow load-balancing on individual radios. **Description —** When using the auto-ap feature, it is not possible to set all of the AP attributes. Per AP load-balancing control is not supported on auto-ap. The system global settings for load-balancing apply to all auto-aps. **Workaround —** If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.
Using telnet over a WAN link may affect the telnet session. **Description —** When using telnet to manage a RAS over a high-latency WAN link, it is possible for the telnet session to stop responding. **Workaround —** Restart the telnet session.
Auto-aps do not behave correctly on cluster seed when the maximum number of APs is configured. **Description —** When a cluster seed RAS boots an auto-ap, it checks the seed configuration on the RAS to determine if the cluster can support any additional APs. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly. **Workaround —** Reduce the number of configured APs in the cluster configuration.
Voice handsets can be sensitive to changes on an in-service SSID. **Description —** Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information. **Workaround —** When using affected handsets, disable the Service Profile prior to making any configuration changes.
The time and date do not synchronize with an NTP server, if the NTP client on the RAS is enabled before the NTP service is started on the server.

Firmware Release 7.0.3.7:
Description — If you reload a switch configuration with cluster mode turned on, RASM cannot determine which RoamAbout switch is the active seed in the cluster configuration. (53952) **Workaround —** Disable cluster mode and then re-enable it. Normal operation resumes on the network.
Using the auto-ap feature does not allow load-balancing on individual radios. (53331) **Description —** When using the auto-ap feature, it is not possible to set all of the AP attributes. Per AP load-balancing control is not supported on auto-ap. The system global settings for load-balancing applies to all auto-aps. (53331) **Workaround —** If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.
Using telnet over a WAN link may affect the telnet session. (52853) **Description —** When using telnet to manage a RoamAbout switch over a high-latency WAN link, it is possible for the telnet session to stop responding. (52853) **Workaround —** Restart the telnet session.
Auto-aps do not behave correctly on cluster seed when the maximum number of APs is configured. (52633) **Description —** When a cluster seed RoamAbout switch boots an auto-ap, it checks the seed configuration on the RoamAbout switch to determine if the cluster can support any additional APs. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly. **Workaround —** Reduce the number of configured APs in the cluster configuration.
CAPWAP data plane UDP port changed from 5001 to 5247. (53029) **Description —** The UDP port for CAPWAP data packets has changed from 5001 to 5247 to comply with the updated CAPWAP specification. You may experience problems with roaming VLANs between RoamAbout switches with MSS Version 7.0 and RoamAbout switches with earlier versions of MSS. **Workaround —** If your network configuration requires tunnled VLANs, be sure that all RoamAbout switches on the network are configured with the same version of MSS.
Using the active-scan feature triggers packet loss on legacy APs with older Intel wireless adaptors. (50901) **Description —** When using active-scan on legacy APs with the Intel 2915 wireless adaptor, a station may experience some level of packet loss. (50901) **Workaround —** Disable active-scan on any legacy APs supporting older Intel clients.

Firmware Release 7.0.3.7:
Voice handsets can be sensitive to changes on an in-service SSID. (41603) **Description —** Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information. **Workaround —** When using affected handsets, disable the Service Profile prior to making any configuration changes.
The time and date do not synchronize with an NTP server, if the NTP client on the RoamAbout switch is enabled before the NTP service is started on the server. (20382)

Firmware Release 6.0.7.2:
There is an open issue where the IfOutOctets MIB query returns a decremented number. This will be resolved in version 7.0.3.7 and higher
IPv6 clients cannot authenticate using Web Portal. This issue affects Web Portal authentication only. The other authentication types (802.1X, MAC, and Last Resort) can be used with IPv6 clients.
If a TRPZ-MP-422 is configured with a transmission power less than 10, wireless clients cannot connect to the AP.
The time and date do not synchronize with an NTP server, if the NTP client on the RAS is enabled before the NTP service is started on the server.
With Direct Path Forwarding enable. In some instances, an error message containing "SSR setup failed.mac" and a multicast address message can all be ignored.
Using a large number of debug trace facilities under certain network conditions can cause access points to become unresponsive. This will result in an access point reset. Please consult GTAC Support Engineering before turning any trace commands on.
Some APs may not respond to the Probe requests from the VoIP handset. This problem occurs only in 802.11b mode. The problem can be solved by disabling and enabling the radio or by changing the access points transmit power settings.
A receive buffer overflow issue was found on the Intel 2100 B/G series wireless client cards when trying to transfer large files (10mb) or larger across the network. The NIC would reset its connection and then reattach to the network during the file transfer. To resolve this issue, create an SSID for the Intel cards only and set a static COS setting to 1 which will throttle the traffic to the Intel 2100 client. Example: set service-profile intel-2100 static-cos enable set service-profile intel-2100 cos 1
In 6.0.x versions of the RAS firmware, use the sticker MAC address on the AP when monitoring that AP with a management application. In a thin mode configuration, when an Enterasys RBT-1002, RBT-3000, or RBT-4102 access point first boots up, the RAS assigns to that AP the AP's sticker MAC address and 16 additional MAC addresses. The switch may not number the 16 MAC addresses sequentially beginning with the AP's sticker MAC address.

Firmware Release 6.0.7.2:

Upgrading to RAS Version 6.0 and Certificate Issue: Customers may experience issues with Certificates or Private keys installed on RASes after upgrading to newer 5.0 and 6.0 releases. Error messages relating to this issue may include the following:

```
   - HTTPD Aug 14 16:32:13.648823 ERROR HTTPD: SSL connection failure (bad cert?);
     - Admin client 145.36.245.51 EAP Aug 14 16:32:14.110502 ERROR EAP_STORE_ERR: No EAP
key pair. Cannot do PEAP
```

Affected services may include SSH, Web-portal, PEAP-offload, WebView, and RASM administrative access and/or Domain Security.

You can prevent this issue by generating new private keys and any related Certificates prior to upgrading to a newer version of the RAS. Third party Certificates should be exempt from this issue provided a new private key was explicitly generated before the CSR request generation. If you are unsure whether a new private key was generated before the initial CSR, the best course of action may be to request a replacement certificate from your provider using a new private key.

Customers encountering this issue can follow the same process to restore normal operation. Details on generating private keys, self-signed Certificates and certificate requests can be found in the Enterasys RoamAbout Mobility System Software Configuration Guide.

The set ap <apnum> boot-configuration switch switch-ip cannot be set at the same time as set ap <apnum> boot-configuration switch name <switch-name> dns <ip addr>. The commands overwrite each other when used.

The Web-portal ACL does not work with IPv6 traffic. IPv6 clients cannot authenticate using Web Portal unless the clients also run IPv4. This issue affects Web-Portal authentication only. The other authentication types (802.1X, MAC, and Last Resort) can be used with IPv6 clients.

The LED radio designation for the RBT-4102-thin is not the same as the RBT-4102 in a standalone mode. In the thin mode, the LED labeled “1” should be associated with the B/G band, and LED “2” is associated with the “A” radio band.

In the RAS User Guides and Configuration manuals, the syntax for the ‘set dap boot-ip’, ‘set dap boot-switch’, and ‘set dap boot-vlan’ commands is incorrect. The actual commands in the RAS firmware version 5.0 are ‘set dap boot-configuration ip’, ‘set dap boot-configuration switch’, and ‘set dap boot-configuration vlan’. In 6.0.x.x, these commands are ‘set ap boot-configuration ip’, ‘set ap boot-configuration switch’, and ‘set ap boot-configuration vlan’.

There is an LED issue with the RBT-82x0 switches, where both ports could show an incorrect connection status after a device reboot when there is no cable attached. This does not affect the performance for either port in any way.

Router redundancy protocol on intermediary devices between RBT-8xx0 switches in a Mobility Domain can interfere with communication among the switches. The workaround to this issue is to set the FDB timer (default 300 seconds) and the ARP timer (default 1200 seconds) to the same values on the RASes. Enterasys Networks recommends using 300 seconds as the value for both timers.

Mixing Autonegotiation with full-duplex mode on a link causes slow throughput and can cause an RBT-8xx0 port to stop forwarding. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to an RBT-8xx0 port in such a configuration can cause forwarding on the link to stop.

The RAS allows ** to be specified as a MAC address glob, but this is invalid for MAC globs.

There is an open issue when deploying the command “set port disable 1” does not disable the port on the RBT-8100.

The RBT-8400 mishandles fragmented packets from the XSR router due to a limitation in the network processor.

Clients using the RBTBG/RBTBJ wireless client card with the RBTBX-PC wireless PCI NIC adapter have experienced extended periods of traffic loss (up to 33% ping loss over a ten-minute time span).

The external antenna names for the RBT-1602 AP have not been converted to the Enterasys specific naming convention. **Note:** Refer to the Tech Tip on page 22 for important information about configuring antenna types for an RBT-1602 Access Point.

Firmware Release 6.0.7.2:
If a location policy (ACL) is added to an SSID that is using Web Authentication, the preconfigured portal ACL will be overwritten and fail to load the logon page. It is strongly recommended not to adjust settings on the preconfigured web portal ACL.
Disabling the dot1x authcontrol function may cause authentication issues. This is a global setting, reaching many portions of the authentication code. It should remain enabled at all times unless specifically directed to disable it. This does NOT turn on dot1x on any of the SSIDs.
ACL names can contain special characters (/,\,-,_), but they cannot contain spaces. ACL names must also begin with a letter and not a number.
Due to a hardware limitation for the RBT3K, the lowest achievable power setting is 10 dB (lowest setting).
The RBT-8400 4 front panel ports are 1Gb ports copper or fiber (default) only.
The unmanaged RBT3K (fat-AP) may encounter conversion upgrade issues to managed mode (thin-AP) across a routed network.
A single "*" used for User Glob does not work when using TLS.
WEP keys cannot be entered in ASCII format. HEX format is currently the only supported input.
The RBT-1002 does not support the automatic generation of RSA values (fingerprints). The dynamic creation of the fingerprint occurs on Access Points that are 'fat-to-thin' conversion types.

For the most up-to-date information concerning known issues, go to the **Global Knowledgebase** section at http://www.enterasys.com/support/. To report an issue not listed in this document or in the **Global Knowledgebase**, contact our Technical Support Staff.

Tech Tip for Choosing External Antenna Types for the RBT-1602 (AP ID: AP1602 & AP1602C) and TRPZ-MP-422 (AP ID: MP422 & MP422A)

When you select an antenna type for the RBT-1602 and TRPZ-MP-422, the menu choices that are displayed are listed in the left-hand column in the table below. Use the antenna part numbers listed in the right-hand column to identify the correct menu choice.

RASM/RBT Antenna Choice:	Enterasys Antenna Part Number:
ANT1060	RBTES-BG-S1060
ANT1120	RBTES-BG-S07120
ANT1180	RBTES-BG-S06180
ANT5060	RBTES-AW-S1460
ANT5120	RBTES-AW-S12120
ANT5180	RBTES-AW-S10180

Tech Tip for the Channel availability for the new DFS2 model Access Points

DFS2 compliant Access Points support fewer channels than non-DFS2 compliant Access points.

Channel availability is based on the AP ID of the installed Access Point. An Access Point with the character of “A “ or “C” on AP ID label denotes a DFS2 compliant device. The country of operation and regulatory domain determine exactly what channels are available for use.

IETF STANDARDS PROTOCOL SUPPORT:

Groups Supported	RFC No. / Title	Description
Security and AAA	RFC 2246	Transport Layer Security (TLS)
	RFC 2284	EAP
	RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5

Groups Supported	RFC No. / Title	Description
	RFC 2548	Microsoft RADIUS VSAs
	RFC 2716	PPP EAP-TLS Authentication Protocol
	RFC 2759	Microsoft PPP CHAP Extensions, Version 2
	RFC 2865	RADIUS Authentication
	RFC 2866	RADIUS Accounting
	RFC 2868	RADIUS Attributes for Tunnel Protocol Support
	RFC 2869	RADIUS Extensions
	RFC 2986	PKCS #10: Certification Request Syntax Specification Version 1.7
	RFC 3580	IEEE 802.1X RADIUS Guidelines
	RFC 3546	Transport Layer Security (TLS) Extensions
	draft-josefsson-pppext-eap-tls-eap	Protected EAP Protocol (PEAP)
	draft-kamath-pppext-peapv0-00.txt	Microsoft PEAP
	draft-kamath-pppext-eap-mschapv2	Microsoft EAP
	CHAP extensions v2	
IEEE	IEEE Std 802.1X-2001	Port-Based Network Access Control
	IEEE Std 802.11i	Enhanced Security for 802.11 Wireless Networks Based on AES
	IEEE Std 802.11h	
	IEEE Std 802.11d	
Encryption	WEP and TKIP: RC4 40-bit and 104-bit	
	SSL and TLS: RC4 128-bit and RSA 1024-bit and 2048-bit	
	CCMP: AES 128-bit (FIPS-197)	
General	RFC 1122 Host Requirements	
	RFC 1393 Traceroute	
	RFC 1519 CIDR	
	RFC 1591 DNS (client)	
	RFC 1769 SNTP	
	RFC 768 UDP	
	RFC 783 TFTP	
	RFC 791 IP	
	RFC 792 ICMP	
	RFC 793 TCP	
	RFC 826 ARP	
	IEEE 802.1D Spanning Tree	
	IEEE 802.1Q VLAN Tagging	
	IEEE 802.3ad (Static Config)	
IP Multicast	RFC 1112 IGMPv1	
	RFC 2236 IGMPv2	
	draft-ietf-idmr-igmp-mrdisc-09.txt	
	draft-ietf-magma-snoop-05.txt	
Quality of Service	RFC 2472 DiffServ Precedence	
	RFC 2597 DiffServ Assured Forwarding	
	RFC 2598 DiffServ Expedited Forwarding	

STANDARD MIB SUPPORT:

NOTE: MIB support for the RoamAbout System is for monitoring only.

RFC No:	Title:
RFC 1213	RFC1213-MIB
RFC 2863	IF-MIB
RFC 1493	BRIDGE-MIB
RFC 2674	Q-BRIDGE-MIB
RFC 2620	RADIUS-ACC-CLIENT-MIB
RFC 2618	RADIUS-AUTH-CLIENT-MIB
RFC 3418	SNMPv2-MIB

ENTERASYS NETWORKS PRIVATE ENTERPRISE MIB SUPPORT:

Title:	Title:
rbtws-system-mib	rbtws-basic-mib
rbtws-trap-mib	rbtws-ap-tc
rbtws-root-mib	rbtws-ap-status
rbtws-port-mib	rbtws-registration-mib
rbtws-info-rf-detect-mib	rbtws-client-session-mib
rbtws-external-server-mib	rbtws-client-session-tc

RADIUS STANDARD AND EXTENDED ATTRIBUTES SUPPORT:

For more information on the supported RADIUS attributes, please refer to the appendix entitled “Supported RADIUS Attributes” in the *Mobility System Software Configuration Guide.*

For more information on assigning authorization attributes, please refer to the chapter entitled “Configuring AAA for Network Users” in the *Mobility System Software Configuration Guide*.

RADIUS Authentication and Authorization Attributes

Attribute:	RFC Source:
Called-Station-Id	RFC2865, RFC3580
Calling-Station-Id	RFC2865, RFC3580
CHAP-Password	RFC2865
Class	RFC2865
Event-Timestamp	RFC2869
Filter-Id	RFC2865, RFC3580
NAS-Identifier	RFC2865, RFC3580
NAS-IP-Address	RFC2865, RFC3580
NAS-Port-Id	RFC2865, RFC3580
Reply-Message	RFC2865
Service-Type	RFC2865, RFC3580
Session-Timeout	RFC2865, RFC3580
State	RFC2865
Tunnel-Private-Group-ID	RFC3580
User-Name	RFC2865, RFC3580
User-Password	RFC2865

Attribute:	RFC Source:
Vendor-Specific	See table below

RADIUS Accounting Attributes

Attribute:	RFC Source:
Acct-Authentic	RFC2866
Acct-Delay-Time	RFC2866
Acct-Input-Gigawords	RFC2866
Acct-Input-Octets	RFC2866
Acct-Input-Packets	RFC2866
Acct-Multi-Session-Id	RFC2866
Acct-Output-Gigawords	RFC2866
Acct-Output-Octets	RFC2866
Acct-Output-Packets	RFC2866
Acct-Session-Id	RFC2866
Acct-Session-Time	RFC2866
Acct-Status-Type	RFC2866

Vendor Specific Attributes

Attribute:	Type, Vendor ID, Vendor Type:
VLAN-Name	26, 14525, 1
Mobility-Profile	26, 14525, 2
Encryption-Type	26, 14525, 3
Time-Of-Day	26, 14525, 4
SSID	26, 14525, 5
End-Date	26, 14525, 6
Start-Date	26, 14525, 7
URL	26, 14525, 8

SNMP TRAP SUPPORT:

SNMP Trap	Description
APBootTraps	Generated when an access point boots.
APTimeoutTraps	Generated when an access point fails to respond to the RoamAbout Switch.
AuthenTraps	Generated when the RoamAbout Switch’s SNMP engine receives a bad community string.
AutoTuneRadioChannelChangeTraps	Generated when the RF Auto−Tuning feature changes the channel on a radio.
AutoTuneRadioPowerChangeTraps	Generated when the RF Auto-Tuning feature changes the power setting on a radio.
ClientAssociationFailureTraps	Generated when a client’s attempt to associate with a radio fails.
ClientAuthorizationSuccessTraps	Generated when a client is successfully authorized.
ClientAuthenticationFailureTraps	Generated when authentication fails for a client.
ClientAuthorizationFailureTraps	Generated when authorization fails for a client.
ClientClearedTraps	Generated when a client’s session is cleared.
ClientDeAssociationTraps	Generated when a client is dissociated from a radio.

SNMP Trap	Description
ClientDot1xFailureTraps	Generated when a client experiences an 802.1X failure.
ClientRoamingTraps	Generated when a client roams.
CounterMeasureStartTraps	Generated when MSS begins countermeasures against a rogue access point.
CounterMeasureStopTraps	Generated when MSS stops countermeasures against a rogue access point.
DAPConnectWarningTraps	Generated when an AP whose fingerprint has not been configured in MSS establishes a management session with the switch.
DeviceFailTraps	Generated when an event with an Alert severity occurs.
DeviceOkayTraps	Generated when a device returns to its normal state.
LinkDownTraps	Generated when the link is lost on a port.
LinkUpTraps	Generated when the link is detected on a port.
MichaelMICFailureTraps	Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
MobilityDomainJoinTraps	Generated when the RoamAbout Switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.
MobilityDomainTimeoutTraps	Generated when a timeout occurs after a RoamAbout Switch has unsuccessfully tried to communicate with a seed member.
PoEFailTraps	Generated when a serious PoE problem, such as a short circuit, occurs.
RFDetectAdhocUserTraps	Generated when MSS detects an ad-hoc user.
RFDetectRogueAPTraps	Generated when MSS detects a rogue access point.
RFDetectRogueDisappearTraps	Generated when a rogue access point is no longer being detected.
RFDetectClientViaRogueWiredAPTraps	Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
RFDetectDoSPortTraps	Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.
RFDetectDoSTraps	Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
RFDetectInterferingRogueAPTraps	Generated when an interfering device is detected.
RFDetectInterferingRogueDisappearTraps	Generated when an interfering device is no longer detected.
RFDetectSpoofedMacAPTraps	Generated when MSS detects a wireless packet with the source MAC address of an Enterasys AP, but without the spoofed AP’s signature (fingerprint).
RFDetectSpoofedSsidAPTraps	Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.
RFDetectUnAuthorizedAPTraps	Generated when MSS detects the MAC address of an AP that is on the attack list.
RFDetectUnAuthorizedOuiTraps	Generated when a wireless device that is not on the list of permitted vendors is detected.

SNMP Trap	Description
RFDetectUnAuthorizedSsidTraps	Generated when an SSID that is not on the permitted SSID list is detected.
ApNonOperStatusTraps	Generated to indicate an AP radio is nonoperational.
ApOperRadioStatusTraps	Generated when the status of an AP radio changes.

GLOBAL SUPPORT:

By Phone: 978-684-1000
1-800-872-8440 (toll-free in U.S. and Canada)

For the Enterasys Networks Support toll-free number in your country:
http://www.enterasys.com/support/

By Email: support@enterasys.com

By Web: http://www.enterasys.com/support/

By Fax: 978-684-1499

By Mail: Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810 (USA)

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Enterasys Networks Support web site.